IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Before the Board of Patent Appeals and Interferences

In re Patent Application of: WATT et al
Atty Dkt. SCS-550-471
C# M#
TC/A.U.: 2183
Serial No. 10/714,483
Examiner: B. Johnson
Filed: November 17, 2003
Date: April 26, 2007
Title: MONITORING CONTROL FOR MULTI-DOMAIN PROCESSORS

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

☐ **Correspondence Address Indication Form Attached.**

☐ **NOTICE OF APPEAL**
Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the Examiner twice/finally rejecting applicant's claim(s). $500.00 (1401)/$250.00 (2401) $

☒ An appeal **BRIEF** is attached in the pending appeal of the above-identified application $500.00 (1402)/$250.00 (2402) $ 500.00

☐ Credit for fees paid in prior appeal without decision on merits -$ ( )

☐ A reply brief is attached. **(no fee)**

☐ Petition is hereby made to extend the current due date so as to cover the filing date of this paper and attachment(s)
One Month Extension $120.00 (1251)/$60.00 (2251)
Two Month Extensions $450.00 (1252)/$225.00 (2252)
Three Month Extensions $1020.00 (1253/$510.00 (2253)
Four Month Extensions $1590.00 (1254/$795.00 (2254) $

☐ "Small entity" statement attached.

Less month extension previously paid on -$( )

TOTAL FEE ENCLOSED $ 500.00

Any future submission requiring an extension of time is hereby stated to include a petition for such time extension. The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our **Account No. 14-1140.** A duplicate copy of this sheet is attached.

901 North Glebe Road, 11th Floor
Arlington, Virginia 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100
SCS:kmm

NIXON & VANDERHYE P.C.
By Atty: Stanley C. Spooner, Reg. No. 27,393

Signature: _____

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of	Confirmation No.: 6434
WATT et al	Atty. Ref.: 550-471
Serial No. 10/714,483	Group: 2183
Filed: November 17, 2003	Examiner: B. Johnson

For: MONITORING CONTROL FOR MULTI-DOMAIN PROCESSORS

* *

APPEAL BRIEF

On Appeal From Group Art Unit 2183

Stanley C. Spooner
NIXON & VANDERHYE P.C.
11th Floor, 901 North Glebe Road
Arlington, Virginia 22203
(703) 816-4028
Attorney for Appellant

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of

WATT et al — Atty. Ref.: 550-471

Serial No. 10/714,483 — Group: 2183

Filed: November 17, 2003 — Examiner: B. Johnson

For: MONITORING CONTROL FOR MULTI-DOMAIN PROCESSORS

* *

April 26, 2007

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

I. REAL PARTY IN INTEREST

The real party in interest in the above-identified appeal is ARM Limited by virtue of an assignment of rights from the inventors to ARM Limited recorded August 20, 2004 at Reel 15714, Frame 905.

II. RELATED APPEALS AND INTERFERENCES

There are believed to be no related appeals, interferences or judicial proceedings with respect to the present application, other than the Pre-Appeal Brief Request for Review previously filed in this appeal.

III. STATUS OF CLAIMS

Claims 1-39 stand rejected in the Final Official Action. The Examiner contends that claims 1-8, 11-16, 18-36, 38 and 39 are unpatentable under 35 USC §103 over Alverson (U.S. Patent 7,020,767) in view of Angelo (U.S. Patent 6,581,162). The Examiner also contends that claims 9, 10, 17 and 37 are unpatentable under 35 USC §103 over the Alverson/Angelo combination in view of "common art." The above rejections of claims 1-39 are appealed.

IV. STATUS OF AMENDMENTS

No further response has been submitted with respect to the Final Official Action in this application other than the filing of a Pre-Appeal Brief Request for Review, which decision was mailed March 28, 2007.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' specification and figures provide an explanation of the claimed invention set out in independent claims 1 and 20, with each claimed structure and method step addressed as to its location in the specification and if illustrated in the figures.

"1. A method of controlling a monitoring function of a processor [10 as shown in Fig. 1 and discussed on page 15, line 8 to page 17, line 10 and elsewhere

in the specification], said processor being operable in at least two domains [secure and non-secure as shown in Fig. 2 and discussed on page 17, lines 12-30 and elsewhere in the specification], comprising a first domain and a second domain, said first and second domains each comprising at least one mode [non-secure mode applications 522 and 524 and secure mode applications 512, 514, 516 shown in Fig. 59 and discussed on Page 106, line 24 to page 107, line 11 and elsewhere in the specification], said method comprising the steps of:

controllably monitoring said processor operating in each of said at least two domains [discussion with respect to Fig. 59 on page 106, line 24 to page 109, line 24 and elsewhere in the specification],

setting at least one control value, said at least one control value relating to a condition and being indicative of whether said monitoring function is allowable in said first domain [discussion with respect to Figs. 61 & 67 on page 109, lines 1-24 and elsewhere in the specification];

allowing initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that said monitoring function is allowable [discussion with respect to Fig. 61 on page 109, lines 1-24 and elsewhere in the specification]; and

not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value indicates that said

control logic [620 as shown in Fig. 68 and discussed on page 112, line 30 – page 113, line 16 and elsewhere in the specification] operable to control initiation of said monitoring logic and to allow initiation of said monitoring logic in said first domain when said condition is present if its related control value indicates that operation of said monitoring logic is allowable, and not to allow initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that operation of said monitoring logic is not allowable ."

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-8, 11-16, 18-36, 38 and 39 stand rejected under 35 USC §103 as unpatentable over Alverson (U.S. Patent 7,020,767) in view of Angelo (U.S. Patent 6,581,162).

Claims 9, 10, 17 and 37 stand rejected under 35 USC §103 as unpatentable over Alverson/Angelo "in view of common art."

VII. ARGUMENT

Appellants' arguments include the fact that the burden is on the Examiner to first and foremost properly construe the language of the claims to determine what structure and/or method steps are covered by that claim. After proper construction of the claim language, the burden is also on the Examiner to

monitoring function is not allowable [discussion with respect to Fig. 61 on page 109, lines 1-24 and elsewhere in the specification]."

"20. A processor [10 as shown in Fig. 1 and discussed on page 15, line 8 to page 17, line 10 and elsewhere in the specification] operable in a first domain and a second domain [secure and non-secure as shown in Fig. 2 and discussed on page 17, lines 12-30 and elsewhere in the specification] said first and second domains each comprising at least one mode [non-secure mode applications 522 and 524 and secure mode applications 512, 514, 516 shown in Fig. 59 and discussed on Page 106, line 24 to page 107, line 11 and elsewhere in the specification], said processor comprising:

monitoring logic [ETM 22 and JTAG controller 18 as shown in Fig. 1 and discussed on page 15, lines 8-30 and elsewhere in the specification] for controllably monitoring said processor operating in each of said first and second domains;

a storage element [CP14 as shown in Fig. 67 and discussed on page 109, lines 1-24 and elsewhere in the specification] operable to be set to contain at least one control value, said at least one control value relating to a condition and being indicative of whether operation of said monitoring logic is allowable in said first domain [discussion with respect to Fig. 61 on page 109, lines 1-24; and

demonstrate where a single reference (in the case of anticipation) or a plurality of references (in the case of an obviousness rejection) teaches each of the structures and/or method steps recited in independent claims 1 and 20.

Furthermore, the Court of Appeals for the Federal Circuit has stated in the case of *In re Rouffet*, 47 USPQ2d 1453, 1458 (Fed. Cir. 1998)

> to prevent the use of hindsight based on the invention to defeat patentability of the invention, this court **requires** the examiner to show a **motivation** to combine the references that create the case of obviousness. In other words, the Examiner **must show reasons** that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. (Emphasis added).

A. The Examiner fails to identify any portion of the Angelo reference which discloses the step of "setting" in claim 1 or the "storage element" of claim 20

Appellants' independent method claim 1 recites the step of "setting at least one control value, said at least one control value relating to a condition . . . ." Similarly, claim 20 recites a storage element for accomplishing the same step. To support a rejection of independent claims 1 and 20 and claims dependent thereon, it is incumbent upon the Examiner to establish where this is taught in the cited references.

The Examiner alleges that this is generally disclosed somewhere in the Angelo reference (the numerous citations on page 3 of the Final Rejection are to the

Angelo reference). On page 3 of the Action, the Examiner suggests that the claimed "setting" step in claim 1 and "storage element" in claim 20 are taught in Angelo at column 7, lines 56-58 and that column 7, line 61 to column 8, line 4 teaches that the control value is related to a condition (also required by claims 1 and 20). From a detailed review of columns 7 and 8, it appears the Examiner is contending that the System Management Interrupt (SMI) is the claimed "control value."

A review of Angelo at columns 7 and 8 indicates that the SMIs which are asserted is a "non-maskable interrupt" having nothing to do with anything "relating to a condition" as in the current claims. There is no reference to a "condition" or suggestion that anything in Angelo is dependent upon recognition of a "condition."

Additionally, there seems to be no stated indication by the Examiner as to how or why he believes the SMI is related to or discloses the claimed "condition." Furthermore, there is no discussion in Angelo that discloses or even suggests that the SMI is "indicative of whether said monitoring function is allowable in said first domain."

As a result of the above, neither of the two aspects specified by Appellants' "setting" step (claim 1) or "storage element" (claim 20) is disclosed in Angelo, i.e., neither (a) the control value being related to a "condition" nor (b) "being indicative of whether said monitoring function is allowable in said first domain." Because the Examiner fails to identify where either of these features positively recited in

independent claims 1 and 20 are present in the Angelo reference, there is no support for the rejection of claims 1-39 under 35 USC §103 and the rejection fails.

B. In view of the Examiner's admission, the Alverson/Angelo combination fails to disclose the claimed "control value"

On page 2 of the Final Rejection, the Examiner admits that Alverson "fails to disclose particular information about monitoring." The above paragraph relating to Error #1 notes that Angelo contains no disclosure of Appellants' "control value" setting step or storage element. Therefore, the combination of Alverson and Angelo fails to contain any disclosure of this claimed element.

In a combination rejection, a claimed element must be disclosed in at least one of the cited references. Here, because the Examiner admits the "control value" is not disclosed in Alverson and because he provides no identification of where this is taught in Angelo, it is clear that the Examiner has failed to meet his burden of proof. The combination of Alverson and Angelo does not disclose the claimed "control value" and thus, if neither reference show the claimed subject matter, it cannot render obvious the subject matter of independent claims 1 and 20 or claims dependent thereon.

Therefore, any further rejection over the combination under 35 USC §103 is respectfully traversed.

C. There is no allegation that either Alverson or Angelo teaches the claimed "not allowing" step in claim 1 or the similar portion of the "control logic" of claim 20

Appellants' claims 1 and 20 also recite the requirement of "not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value indicates that said monitoring function is not allowable." The Examiner quotes this claim language (at the end of page 3 in the official action) and alleges that this claimed feature is disclosed in Angelo (column 7, line 61 to column 8, line 4).

However, a review of the cited portion of Angelo contains no language or suggestion even vaguely related to "not allowing initiation of said monitoring function . . . ." Why or how the Examiner believes the "not allowing" or "control logic" of the claims is hidden somewhere in Angelo is not apparent from the Official Action.

As set out by the Court of Appeals for the Federal Circuit, "[t]he PTO has the burden under section 103 to establish a *prima facie* case of obviousness." (Emphasis in original). *In re Fine*, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). The PTO "can satisfy this burden only by showing some objective teaching in the prior art . . . ." *Id.* Here, the Examiner has simply failed to provide any such identification of any teaching in the Alverson/Angelo references of the claimed elements and steps and therefore any further rejection under 35 USC §103 is respectfully traversed.

D. The Examiner appears to ignore the fact that the Angelo "teaches away" from Appellants' independent claims

Appellants' independent claims specify the above-noted step of "not allowing" the monitoring function when the "condition" is present and the related "control value" indicates that the monitoring function is not allowable. Contrarily, Angelo teaches that its monitoring function (i.e., entry into the System Management Mode (SMM)) is **always** allowed in response to an SMI (the Examiner appears to contend that the SMI is analogous to the claimed "control value"). Because Angelo teaches that the monitoring function is **always** allowed, it would necessarily lead those of ordinary skill in the art **away** from Appellants' **conditional non-allowance** and thereby lead away from the combination of elements asserted by the Examiner.

As a result, the non-obviousness of Appellants' claimed subject matter is believed established, especially in view of the Alverson and Angelo teachings and under 35 USC §103.

E. The Examiner provides no support for his "common art" rejection of claims 9, 10, 17 and 37

Claims 9, 10, 17 and 37 stand newly rejected under 35 USC §103 as unpatentable over the Alverson/Angelo combination "in view of common art" (page 11 of the Final Rejection). Because these claims depend from claims 1 and

20, each of the above-noted errors is applicable to these claims with respect to the Alverson/Angelo combination and is incorporated by reference.

The Examiner's additional admission that "Angelo fails to particularly disclose that the information includes instruction traces" is very much appreciated (page 11). However, the Examiner's assertion that "saving instruction traces is common in the art and can be utilized for many debugging purposes" is respectfully traversed.

As noted in the Manual of Patent Examining Procedure (MPEP) Section 2144.03, "if the applicant traverses such an assertion [of official notice of facts outside of the record] the examiner should cite a reference in support of his or her position." While this new rejection was only recently instituted in the Final Rejection (even though claims 9, 10, 17 and 37 are in their originally filed form), the burden is on the Examiner to establish some prior art disclosure if his contention is traversed. Appellants respectfully traverse the Examiner's contention and had no previous opportunity to respond to the contention, since it was not raised until the Final Rejection.

Accordingly, the Examiner's rejection of claims 9, 10, 17 and 37 is traversed as being unsupported by the admitted defects in the Alverson and Angelo references and the Examiner's failure to cite any "common art" supportive of the Examiner's position.

F. The rejection of claims 1-8, 11-16, 18-36, 38 and 39 under 35 USC §103 over Alverson (U.S. Patent 7,020,767) in view of Angelo (U.S. Patent 6,581,162) is in error for numerous reasons

In order to avoid duplication, as sections A through E above relate to the Examiner's rejections, the conclusion reached will be addressed by reference to the section which is incorporated by reference.

The Examiner rejects claims 1-8, 11-16, 18-36, 38 and 39 under 35 USC §103 over Alverson (U.S. Patent 7,020,767) in view of Angelo (U.S. Patent 6,581,162). As noted in section A above, the Angelo reference fails to teach the "setting step" in claim 1 and the "storage element" in claim 20. As in section B, the Examiner admits that Alverson fails to disclose the claimed "control value" and fails to identify where this is disclosed in Angelo. As in section C, the Examiner fails to allege or support the allegation that the claimed "not allowing" step of claim 1 and the "control value" of claim 20 is disclosed in either Alverson or Angelo. As a result, because neither of the combined references contain a teaching of the recited elements or steps, the combination does not support the rejection under 35 USC §103.

Moreover, at no point in the rejections does the Examiner provide the required "reason" or "motivation" (see the above *In re Rouffet* quote) for combining the Alverson and Angelo references.

Finally, as in section D above, Angelo would lead one of ordinary skill in the art away from the claimed invention since it teaches monitoring is always allowed instead of the claimed conditional allowance. Non-obviousness is indicated where a cited prior art reference would lead one of ordinary skill in the art away from the claimed invention.

Any of the above reasons supports the reversal of the Examiner rejection of claims 1-8, 11-16, 18-36, 38 and 39 and the existence of all of the reasons confirms the inappropriateness of the rejection.

G. The rejection of claims 9, 10, 17 and 37 under 35 USC §103 over Alverson/Angelo "in view of common art" is in error for numerous reasons

In order to avoid duplication, as sections A through E above relate to the Examiner's rejections, the conclusion reached will be addressed by reference to the section which is incorporated by reference. In as much as the Alverson/Angelo combination is applied in this rejection, the above comments in section F relating thereto are specifically incorporated by reference.

The Examiner attempts to buttress his rejection of claims 9, 10, 17 and 37 under 35 USC §103 over the Alverson/Angelo combination by reference to a nebulous reference "common art." As noted in section F, the Examiner has not previously recited this basis for rejection and Appellant has specifically traversed this rejection thereby rendering moot the present rejection.

Moreover, the Examiner does not allege that the above deficiencies in Alverson and Angelo are cured by the "common art." Therefore, even if combined, there would be no disclosure of the subject matter of the independent claims 1 and 20 or any claims dependent thereon.

Additionally, the Examiner has provided no "reason" or "motivation" for the Alverson/Angelo/"common art" combination. Further, the Examiner has ignored the Angelo teaching away from the claims.

As a result of the above, it is clear that no *prima facie* basis for the rejection of claims 9, 10, 17 and 37 has been set out by the Examiner and these claims should be allowed.

VIII. CONCLUSION

Neither Angelo or Alverson disclose Appellants' claimed setting of at least one control value. There is no demonstration of how or where the Alverson or Angelo references teach the claimed "not allowing initiation" feature. The Angelo reference specifically teaches away from the claimed feature because it suggests that entry into SMM is always in response to an SMI which the Examiner believes is analogous to Appellants' "control value." The failure to disclose what the Examiner believes to be "common art" is fatal to the rejection of the cited rejected dependent claims. The additional failures to establish a "reason" or "motivation" for combining the references and the failure to appreciate that Angelo teaches

away from the rejection, all combine to confirm the lack of any reasonable basis for rejection of the pending claims.

As a result of the above, there is simply no support for the rejections of Applicants' independent claim or claims dependent thereon under 35 USC §103. Thus, and in view of the above, the rejection of claims 1-39 under 35 USC §103 is clearly in error and reversal thereof by this Honorable Board is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____

Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
Enclosures

IX. CLAIMS APPENDIX

1. A method of controlling a monitoring function of a processor, said processor being operable in at least two domains, comprising a first domain and a second domain, said first and second domains each comprising at least one mode, said method comprising the steps of:

controllably monitoring said processor operating in each of said at least two domains,

setting at least one control value, said at least one control value relating to a condition and being indicative of whether said monitoring function is allowable in said first domain;

allowing initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that said monitoring function is allowable; and

not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value indicates that said monitoring function is not allowable.

2. A method according to claim 1, wherein said first domain is a secure domain and said second domain is a non-secure domain, said processor being operable such that when executing a program in a secure mode within said secure

domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain.

3. A method according to claim 2, wherein said condition comprises a domain, mode or type of monitoring function.

4. A method according to claim 3, wherein said condition comprises a secure domain and said control value comprises a secure domain enable value, initiation of monitoring in said secure domain only being allowed if said secure domain enable value is set.

5. A method according to claim 3, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode.

6. A method according to claim 5 wherein said control value comprises a secure user mode enable bit and initiation of monitoring from secure user mode is only allowed if said secure user mode enable bit has been set.

7. A method according to claim 4, wherein said condition comprises a type of monitoring function.

8. A method according to claim 7, wherein said condition comprises a debug monitoring function and said control value comprises a debug enable bit, initiation of debug in said first domain only being allowable if said debug enable bit has been set.

9. A method according to claim 8, wherein said condition comprises a trace monitoring function and said control value comprises a trace enable bit, initiation of trace in said first domain only being allowable if said control trace enable bit has been set.

10. A method according to claim 9, wherein said secure domain enable value comprises a secure debug enable bit and a secure trace enable bit, initiation of debug and trace in said secure domain only being allowable if respective portions of said secure domain enable value are set.

11 A method according to claim 1, said method comprising setting a plurality of control values, each of said plurality of control values relating to a different condition; and

only allowing initiation of said monitoring function in said first domain if any of said conditions are present if each of said control values related to a condition that is present indicate that said monitoring function is allowable.

12. A method according to claim 1, said method further comprising said steps of:

setting a control indicator, said control indicator indicating that monitoring is only allowable for specified applications; and

prior to initialising said monitoring function checking an application identifier; and

only allowing initiation of said monitoring function if said application currently running is one for which monitoring is allowable.

13. A method according to claim 12, wherein the step of setting a control indicator comprises setting a control indicator stored in a predetermined position in a storage element.

14. A method according to claim 12, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data, said method comprising the further step of:

following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain while an application running on said processor is one for which monitoring is allowable.

15. A method according to claim 1, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data, said method comprising the further step of:

following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain when a condition changes if a control value related to the changed condition indicates that said monitoring function is allowable.

16. A method according to claim 1, wherein setting of at least one control value is performed either by setting said control value via an input port or by setting said control value from the first domain.

17. A method according to claim 16, said method comprising the further step of blocking write access to said control value via said input port such that the step of setting said control value can henceforth only be performed by setting said control value from said first domain.

18. A method according to claim 1, wherein said first domain comprises a first user mode and a first privileged mode and the step of setting at least one control value in said first domain, comprises setting said control value from said first privileged mode.

19. A method according to claim 16, wherein said first domain comprises a first user mode and a first privileged mode and said step of setting at least one control value in the first domain, comprises inputting an authentication code from a mode that is not a first privileged mode and then setting said control value.

20. A processor operable in a first domain and a second domain said first and second domains each comprising at least one mode, said processor comprising:

monitoring logic for controllably monitoring said processor operating in each of said first and second domains;

a storage element operable to be set to contain at least one control value, said at least one control value relating to a condition and being indicative of whether operation of said monitoring logic is allowable in said first domain; and

control logic operable to control initiation of said monitoring logic and to allow initiation of said monitoring logic in said first domain when said condition is present if its related control value indicates that operation of said monitoring logic is allowable, and not to allow initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that operation of said monitoring logic is not allowable.

21. A processor according to claim 20, wherein said first domain is a secure domain and said second domain is a non-secure domain said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain.

22. A processor according to claim 21, wherein said condition comprises a domain, mode or type of monitoring logic.

23. A processor according to claim 22, wherein said condition comprises a secure domain and said control value comprises a secure domain enable bit, initiation of monitoring in said secure domain only being allowed if said storage element contains a secure domain enable bit.

24. A processor according to claim 22, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode.

25. A processor according to claim 24 wherein said control value comprises a secure user mode enable bit and said control logic is operable to allow initiation of said monitoring logic from secure user mode only when said storage element contains a secure user mode enable bit.

26. A processor according to claim 21, wherein said condition comprises a type of monitoring function.

27. A processor according to claim 26, wherein said condition comprises debug monitoring and the control value comprises a debug enable bit, said control logic being operable to allow initiation of said monitoring logic in said first domain only when the storage element contains a debug enable bit.

28. A processor according to claim 26, wherein said condition comprises trace monitoring and said control value comprises a trace enable bit, said control logic being operable to allow initiation of said trace logic in said first domain only when said storage element contains a control trace enable bit.

29. A processor according to claim 20, wherein:

said storage element is operable to contain a plurality of control values, each of said plurality of control values relating to a different condition; and

said control logic is operable to only allow initiation of said monitoring logic in said first domain if any of said conditions are present if each of the control values related to a condition that is present indicate that the monitoring logic is allowable.

30. A processor according to claim 29 wherein one condition comprises a secure domain and a corresponding control value comprises a secure domain enable bit and a further condition comprises a secure user mode and a corresponding control value comprises a secure user mode enable bit, said control logic being operable to initiate said monitoring logic from secure user mode only when said storage element contains both a secure user mode enable bit and a secure domain enable bit.

31. A processor according to claim 20, wherein:

said storage element is further operable to contain a control indicator, said control indicator indicating that monitoring is only allowable for identified applications; and

said control logic is operable to check at least one identifier identifying an application that is allowable, said control logic only initiating said monitoring logic in the first domain when said application currently running is one identified as being one for which monitoring is allowable.

32. A processor according to claim 31, said processor comprising a further storage element, said storage element being operable to contain said at least one identifier specifying an application that is allowable.

33. A processor according to claim 31, wherein said monitoring logic is operable to monitor the processor and capture diagnostic data; and

wherein said control logic is operable to control the monitoring logic to suppress capturing of diagnostic data in said first domain when said control logic detects that said application running is not one identified as being allowable.

34. A processor according to claim 20, said processor further comprising an input port, wherein said control value is operable to be set in said storage element either via the input port or via an input from said first domain.

35. A processor according to claim 34, said processor comprising a means of blocking write access to said control value via said input port such that setting of said control value can henceforth only be performed by setting said control value via an input from said first domain.

36. A processor according to claim 20, wherein said first domain comprises a first user mode and a first privileged mode and said control value is operable to be set in said storage element via an input from said first privileged mode.

37. A processor according to claim 35, wherein said first domain comprises a first user mode and a first privileged mode and said control value is operable to be set in said storage element by input of an authentication code from a mode that is not a first privileged mode followed by an input of said control value.

38. A processor according to claim 20, wherein said storage element comprises a register.

39. A processor according to claim 30, wherein said further storage element comprises a register.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.